(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－186123
（P2001－186123A）
(43)公開日　平成13年７月６日(2001.7.6)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｄ	５Ｊ１０４
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ	５Ｋ０６７

審査請求　未請求　請求項の数２　ＯＬ　（全４頁）

(21)出願番号　特願平11－369415

(22)出願日　平成11年12月27日(1999.12.27)

(71)出願人　000001258
川崎製鉄株式会社
兵庫県神戸市中央区北本町通１丁目１番28号

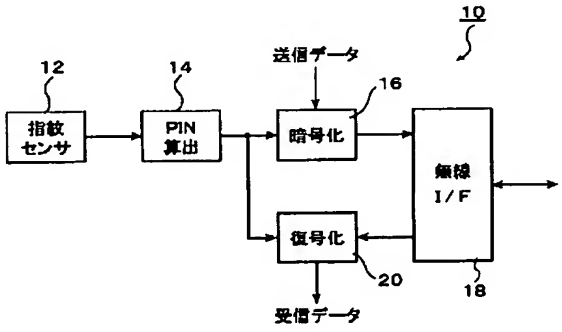
(72)発明者　山本　英明
東京都千代田区内幸町２丁目２番３号　川崎製鉄株式会社東京本社内

(74)代理人　100080159
弁理士　渡辺　望稔　（外１名）

Ｆターム(参考)　5J104 AA01 AA07 KA01 KA17 NA05 PA01
5K067 AA32 DD00 DD17 DD23 EE02 EE25 GG01 GG11 HH22 HH23

(54)【発明の名称】　無線認証方法および認証装置

(57)【要約】
【課題】小型の無線通信機器同士であっても、任意のＰＩＮ（個人識別番号）を設定することができ、このＰＩＮを用いて、両方の無線通信機器を認証することができる無線認証方法および認証装置を提供する。
【解決手段】指紋センサを用いて指紋データを発生し、この指紋データに基づいて個人識別番号を算出し、この個人識別番号を使用して、無線通信機器同士の間でデータを暗号化して送受信することにより、上記課題を解決する。



【特許請求の範囲】
【請求項１】指紋センサを用いて、使用者の指紋を読み取って指紋データを発生し、
この指紋データに基づいて個人識別番号を算出し、
この個人識別番号を使用して送信データを暗号化し、
通信相手の無線通信機器に対して、前記暗号化された送信データを無線送信するとともに、前記通信相手の無線通信機器から送信されてくる暗号化された送信データを受信し、
前記個人識別番号を使用して、前記通信相手の無線通信機器から送信されてくる送信データを復号化して受信データを得ることを特徴とする無線認証方法。
【請求項２】使用者の指紋を読み取って指紋データを発生する指紋センサと、前記指紋データに基づいて個人識別番号を算出するＰＩＮ算出部と、前記個人識別番号を使用して送信データを暗号化する暗号化部と、無線により、通信相手の無線通信機器に対して暗号化された送信データを送信し、前記通信相手の無線通信機器から送信されてくる暗号化された送信データを受信する無線Ｉ／Ｆ部と、前記個人識別番号を使用して、前記通信相手の無線通信機器から送信されてくる送信データを復号化して受信データを得る復号化部とを備えていることを特徴とする無線認証装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、小型の無線通信機器同士の間で両者の認証を行う無線認証方法および無線認証装置に関するものである。
【０００２】
【従来の技術】一般的に、無線に限らず、複数の機器の間で通信を行う場合に両者の認証を必要とする場合がある。例えば、携帯用の情報端末同士で無線通信をする場合、両者の間で認証なしに自由に通信ができるのであれば、第３者にも自由に通信することが可能であるため、両者の間で通信中の情報を第３者に盗まれる危険性がある。特に、無線の場合には傍受が容易であるため、安全性の面から、相互にやり取りするデータを暗号化するのが好ましい。
【０００３】例えば、対称アルゴリズムを使用して暗号化するのであれば、通信する両方の通信機器で同じキーデータを用意し、送信するデータを暗号化するための暗号キーとして、また、受信したデータを復号するための復号キーとして使用する。この時、両者の間で最初に通信を行う前に、まず、共通のキーデータを決定し、これを何らかの方法で通信相手に通知した後、外部から両方の通信機器に入力しておく必要がある。
【０００４】ここで、通信相手の通信機器にキーデータを通知する際に、通信によって両者間でキーデータを交換すると、キーデータを暗号化せずに通信しなければならないために安全性が劣る。また、特定のキーデータを決定せず、デフォルト（初期値）のキーデータを使用して送信データを暗号化すると、悪意のある第３者が、このデフォルトのキーデータを使用して認証を簡単にクリアすることができる。このため、同様に安全性が問題となる。
【０００５】これに対し、Ｂluetooth規格の場合、その「Ｆoundation Core」と呼ばれる設計仕様書第１．０Ａ版の第１０３０ページに示されているように、使用者がＰＩＮ（個人識別番号）を両方の無線通信機器に対して直接入力することにより両者を接続するためのリンクキーを生成する。Ｂluetooth規格とは、短距離通信向けの低価格な次世代無線通信技術であって、２．４ＧＨｚの周波数帯域を利用して、最大約１０ｍの距離で１Ｍｂｐｓのデータ通信が可能なものである。
【０００６】このように、安全性の点からは、ＰＩＮを何らかの形で通信機器に直接入力するのが好ましい。この際、パーソナルコンピュータ等のように、キーボードのような入力装置を備えるものであれば簡単にＰＩＮを入力することができる。しかし、例えば重量やサイズ等の制限によってキーボード等の入力装置を備えることができない小型の通信機器では、使用者が任意のＰＩＮを設定することができず、セキュリティの面で安全性に劣るという問題がある。
【０００７】
【発明が解決しようとする課題】本発明の目的は、前記従来技術に基づく問題点を解消し、小型の無線通信機器同士であっても、任意のＰＩＮを設定することができ、このＰＩＮを用いて、両方の無線通信機器を認証することができる無線認証方法および認証装置を提供することにある。
【０００８】
【課題を解決するための手段】上記目的を達成するために、本発明は、指紋センサを用いて、使用者の指紋を読み取って指紋データを発生し、この指紋データに基づいて個人識別番号を算出し、この個人識別番号を使用して送信データを暗号化し、通信相手の無線通信機器に対して、前記暗号化された送信データを無線送信するとともに、前記通信相手の無線通信機器から送信されてくる暗号化された送信データを受信し、前記個人識別番号を使用して、前記通信相手の無線通信機器から送信されてくる送信データを復号化して受信データを得ることを特徴とする無線認証方法を提供するものである。
【０００９】また、本発明は、使用者の指紋を読み取って指紋データを発生する指紋センサと、前記指紋データに基づいて個人識別番号を算出するＰＩＮ算出部と、前記個人識別番号を使用して送信データを暗号化する暗号化部と、無線により、通信相手の無線通信機器に対して暗号化された送信データを送信し、前記通信相手の無線通信機器から送信されてくる暗号化された送信データを受信する無線Ｉ／Ｆ部と、前記個人識別番号を使用し

て、前記通信相手の無線通信機器から送信されてくる送信データを復号化して受信データを得る復号化部とを備えていることを特徴とする無線認証装置を提供するものである。

【００１０】

【発明の実施の形態】以下に、添付の図面に示す好適実施例に基づいて、本発明の無線認証方法および認証装置を詳細に説明する。

【００１１】図１は、本発明の無線認証装置の一実施例のブロック構成図である。本発明の無線認証装置１０は、バイオメトリクス（生物学的特徴）を利用して、小型の無線通信機器同士がネットワークを動的に構築する際のセキュリティ機能を提供するもので、同図に示すように、指紋センサ１２と、ＰＩＮ（個人識別番号）算出部１４と、暗号化部１６と、無線Ｉ／Ｆ（インターフェース）部１８と、復号化部２０とを備えている。

【００１２】図示例の無線認証装置１０において、まず、指紋センサ１２は、使用者の指紋を読み取り、指紋データとなるデジタル画像データを発生する。指紋センサ１２は、小型軽量のものであればどのような構造のものでもよいが、例えば米Veridicom社や仏・伊ＳＧＳ－Thomson Microelectronics社等が提案するような指紋の静電容量を電子的に計測する半導体指紋センサであるのが好ましい。指紋データは次のＰＩＮ算出部１４に供給される。

【００１３】ここで、上記半導体指紋センサは、スキャナやカメラ等の読み取り装置を使用して光学的ないしは機械的に指紋を読み取るのではなく、１つの半導体チップにより構成された静電容量センサアレイによって、指紋の山と谷により引き起こされる電界の変化を測定して指紋の模様を記録し、指紋を電子的に表現した画像データを生成する。半導体指紋センサは小型軽量であるため、小型の無線通信機器に好適に利用可能である。

【００１４】続いて、ＰＩＮ算出部１４は、指紋センサ１２から供給される指紋データに基づいてＰＩＮを算出する。このＰＩＮは暗号化部１６および復号化部１８の両方に供給される。なお、ＰＩＮを算出する方法は何ら限定されず、従来公知の方法はいずれも利用可能である。ＰＩＮの算出方法については一例を後述する。続いて、暗号化部１６は、ＰＩＮを使用して送信データを暗号化する。暗号化された送信データは無線Ｉ／Ｆ部１８に供給される。

【００１５】無線Ｉ／Ｆ部１８は、無線により、通信相手の無線通信機器に対して暗号化された送信データを送信するとともに、通信相手の無線通信機器から送信されてくる暗号化された送信データを受信する。無線Ｉ／Ｆ部１８によって受信されたデータは復号化部２０へ供給される。最後に、復号化部２０は、ＰＩＮを使用して、通信相手の無線通信機器から送信されてくる暗号化された送信データを復号化し、受信データを得る。

【００１６】次に、上記本発明の無線認証装置１０の動作とともに、本発明の無線認証方法について説明する。なお、以下の説明では、指紋センサ１２として前述の半導体指紋センサを用い、本発明を適用する２台の無線通信機器同士の間で無線通信を行う場合を例に挙げて説明する。

【００１７】本発明の無線認証方法に従って、使用者は、２台の無線通信機器を無線通信が可能な距離に配置し、まず、一方の無線通信機器において、本発明の無線認証装置１０の指紋センサ１２の上に任意の指の腹側を載せて指紋を読み取らせる。この時、指紋センサ１２から、指紋を読み取って得られる１０mm角の画像データが指紋データとして出力され、この指紋データに基づいて、ＰＩＮ算出部１４により、例えば以下の手順に従ってＰＩＮが算出される。

【００１８】まず、指紋データから指紋の渦巻きの中心を求め、渦巻きの中心から半径３mm以内の指紋の山の数Ｎｒ［ｉ］、指紋の谷の数Ｎｅ［ｉ］および指紋の２股の数Ｎｂ［ｉ］を求める。ここで、０≦Ｎｒ［ｉ］≦２５５の整数、０≦Ｎｅ［ｉ］≦２５５の整数、０≦Ｎｂ［ｉ］≦２５５の整数である。また、ｉは何回目の読み取りであるかを表す数字（以下、同じである。）であって、本実施例では０≦ｉ≦９の整数とする。

【００１９】指紋センサ１２によって指紋を読み取り、上記指紋の山の数Ｎｒ［ｉ］、指紋の谷の数Ｎｅ［ｉ］および指紋の２股の数Ｎｂ［ｉ］を求めることを連続して１０回（０≦ｉ≦９）行う。そして、下記算出式（１）に従って、それぞれ指紋の山の数の平均値Ｎｒａ、指紋の谷の数の平均値Ｎｅａおよび指紋の２股の数の平均値Ｎｂａを算出する。このように、平均値を算出することによって、指紋センサ１２による読み取りの誤差を補正することができる。

【００２０】

【数１】

$$Nra=\sum_{i=0}^{9}Nr[i]/10$$

$$Nea=\sum_{i=0}^{9}Ne[i]/10 \qquad \cdots(1)$$

$$Nba=\sum_{i=0}^{9}Nb[i]/10$$

【００２１】最後に、上記指紋の山の数の平均値Ｎｒａ、指紋の谷の数の平均値Ｎｅａおよび指紋の２股の数の平均値Ｎｂａを用い、下記算出式（２）に従って２４ビットの数値を作成し、これをＰＩＮとして使用する。

$$PIN=Nra\times 2^{16}+Nea\times 2^{8}+Nba \quad \cdots \quad (2)$$

なお、１０回の読み取りは、半導体指紋センサであれば１秒以下の時間で終了する。上記の動作が正常終了する

と、使用者にはその旨が指示される。

【００２２】この指示を受けて、使用者は、もう一方の無線通信機器においても同じようにして、本発明の無線認証装置１０の指紋センサ１２の上に同じ指の腹側を載せて指紋を読み取らせる。これにより、２台の無線通信機器には同じＰＩＮが発生される。なお、例えば渦巻きの中心が指紋データの中心から半径２ｍｍ以内に存在していない場合には読み取りのやり直しをするよう指示するなど適宜設定を変更してもよい。

【００２３】その後、発生されたＰＩＮを使用して２台の無線通信機器の間で無線通信を行う。すなわち、暗号化部１６により、発生されたＰＩＮを使用して送信すべきデータが暗号化され、暗号化された送信データは無線Ｉ／Ｆ部１８を通して通信相手の無線通信装置に送信される。また、無線Ｉ／Ｆ部１８を通して通信相手の無線通信装置から暗号化された送信データを受信して、復号化部２０により、ＰＩＮを使用して復号化され、受信データを得る。

【００２４】以上のように、本発明の無線認証方法および認証装置では、小型軽量な指紋センサによって指紋を読み取り、読み取った指紋データに基づいてＰＩＮを算出し、ＰＩＮを使用してデータの暗号化および復号化を行う。従って、本発明の無線認証方法および認証装置は、小型の無線通信機器に好適に利用可能であり、指紋センサの上に指を載せるだけで無線通信機器同士の間の認証を行って安全に無線通信をすることができる。

【００２５】なお、本発明の無線認証装置として、使用者の指紋をあらかじめ読み取って得られる画像データや、この画像データに基づいて算出されたＰＩＮ等を基準データとして格納しておいてもよい。この場合、本発明を適用する無線通信機器を単体で使用する際に、指紋を読み取って得られる画像データやＰＩＮとあらかじめ記憶されている基準データとを比較することによって使用者を認証し、使用可能な使用者を制限することも可能である。

【００２６】本発明の無線認証方法および認証装置は、基本的に以上のようなものである。以上、本発明の無線認証方法および認証装置について詳細に説明したが、本発明は上記実施例に限定されず、本発明の主旨を逸脱しない範囲において、種々の改良や変更をしてもよいのはもちろんである。

【００２７】

【発明の効果】以上詳細に説明した様に、本発明の無線認証方法および認証装置は、指紋センサを用いて指紋データを発生し、この指紋データに基づいてＰＩＮを算出し、このＰＩＮを使用して、無線通信機器同士の間でデータを暗号化して送受信するものである。本発明で用いる指紋センサは小型軽量であるため、本発明の無線認証方法および認証装置によれば、小型の無線通信機器の重量やサイズ等を損ねることなくＰＩＮを取得することができ、指紋センサの上に指を載せるだけで無線通信機器同士の間の認証を行い、安全に無線通信をすることができる。

【図面の簡単な説明】

【図１】　本発明の無線認証装置の一実施例のブロック構成図である。

【符号の説明】

１０　無線認証装置
１２　指紋センサ
１４　ＰＩＮ（個人識別番号）算出部
１６　暗号化部
１８　無線Ｉ／Ｆ（インターフェース）部
２０　復号化部

【図１】